

CLAIMS

1. A method for password-based authentication in a communication system comprising a group (100) of at least two units (12; 22; 32; 42; 52; 72; 82; 92) associated with a common password, **characterized by** the steps of
- 5 assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;
- determining, at a first unit (32-1; 42-1; 52-2; 92-1), a check token for a
- 10 second unit (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) based on the password and the authentication token of the first unit; and
- comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.
- 15
2. The method of claim 1, **characterized by** the further step of
- deleting the password and all significant parameters generated in the authentication procedure except the authentication tokens after usage thereof.
- 20
3. The method of claim 1, **characterized by** the further step of
- accepting, at the second unit (42-2; 52-1, 52-3, 52-4; 92-4) and in response to a successful authentication, update information securely transferred from the first unit (42-1; 52-2; 92-1), at least a portion of the update information being created at the first unit.
- 25
4. The method of claim 3, **characterized in that** the update information is associated with revocation of a non-trusted group member.
5. The method of claim 3, **characterized in that** the update information
- 30 relates to a password change.
6. The method of claim 3, **characterized in that** the update information is selected from the group of: new authentication tokens, a new group key, a

group-defining list, and a revocation list (45; 55; 95), including combinations thereof.

7. The method of claim 3, **characterized by** delegation of update rights to a
5 third intermediate unit (92-2, 92-3), and sending at least a portion of the
update information for the second unit (92-4) to the intermediate unit.

8. The method of claim 7, **characterized in that** the update information is
accompanied by a time stamp for determining whether the update information
10 is still valid when the intermediate unit (92-2, 92-3) encounters the second
unit (92-4).

9. The method of claim 7, **characterized in that** the delegation of update
rights comprises delegation of rights to further delegate update rights.

15

10. The method of claim 1, **characterized in that** the assigning step in turn
comprises the steps of

determining, at an assigning unit (72-1; 82-2) in the group, a token secret
common for the group and non-correlated with the password; and

20 creating, at the assigning unit, the authentication token for another unit
(72-2, 72-3; 82-4) in the group based on the token secret and the password.

11. The method of claim 10, **characterized in that** the step of determining
the token secret involves generating the token secret, as a part of an initial
25 set-up procedure.

12. The method of claim 1, **characterized in that** the step of determining the
check token in turn comprises the steps of

30 retrieving, at the first unit (32-1; 42-1; 52-2; 92-1), the token secret using
the authentication token of the first unit and the password; and

creating, at the first unit, the check token for the second unit (32-2; 42-2;
52-1, 52-3, 52-4; 92-4) based on the token secret and the password.

13. The method of claim 10 or 12, **characterized in that** the creating step involves using a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

5 14. The method of claim 13, **characterized in that** the locking function is a symmetric encryption function.

15. The method of claim 13, **characterized in that** the locking function is implemented through password-based secret sharing.

10

16. The method of claim 1, **characterized by** implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

15 17. The method of claim 1, **characterized by** the further step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

18. The method of claim 1, **characterized by** the further step of sending an
20 authentication response message (34; 44; 94) from the second unit (32-2; 42-2; 92-4) indicating the result of the comparing step.

19. The method of claim 1, **characterized by** further authentication of the second unit (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) towards the first unit (32-1;
25 42-1; 52-2; 92-1), whereby the first and second units are mutually authenticated towards each other.

20. The method of claim 19, **characterized by** the steps of:

generating a respective random value at the first and second unit;

30 determining temporary test secrets at the first and second unit based on the random values; and

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes.

21. The method of claim 1, **characterized in that** critical operations for which authentication is needed are listed in policies in at least one of the units (12; 22; 32; 42; 52; 72; 82; 92).

5

22. The method of claim 3, **characterized in that** a unit (42-2; 52-1, 52-3, 52-4; 92-4) that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

10

23. The method of claim 1, **characterized in that** the group (100) of units constitutes a Personal Area Network (PAN).

24. The method of claim 1, **characterized in that** the authentication tokens
15 are tamper-resistantly stored in the respective units (12; 22; 32; 42; 52; 72; 82; 92).

25. A communication system including a group (100) of at least two units (12; 22; 32; 42; 52; 72; 82; 92) associated with a common password, and
20 means for password-based authentication, **characterized by**

means for assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

25 means for determining, at a first unit (32-1; 42-1; 52-2; 92-1), a check token for a second unit (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) based on the password and the authentication token of the first unit; and

means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.

30

26. The system of claim 25, **characterized by** further comprising

means for deleting the password and parameters generated in the authentication procedure except the authentication tokens after usage thereof.

27. The system of claim 25, **characterized by** further comprising
means for transferring update information from the first unit (42-1; 52-
2; 92-1) to the second unit (42-2; 52-1, 52-3, 52-4; 92-4); and

5 means for accepting, at the second unit, update information from the first
unit in response to a successful authentication.

28. The system of claim 27, **characterized in that** the update information is
associated with revocation of a non-trusted group member.

10 29. The system of claim 27, **characterized in that** the update information
relates to a password change.

30. The system of claim 27, **characterized in that** the update information is
15 selected from the group of: new authentication tokens, a new group key, a
group-defining list, and a revocation list (45; 55; 95), including combinations
thereof.

31. The system of claim 27, **characterized by** means for delegation of update
20 rights to a third intermediate unit (92-2, 92-3), and means for sending at least
a portion of the update information for the second unit (92-4) to the
intermediate unit.

32. The system of claim 25, **characterized in that** the means for assigning in
25 turn comprises

means for determining, at an assigning unit (72-1; 82-2) in the group, a
token secret common for the group and non-correlated with the password;
and

30 means for creating, at the assigning unit, the authentication token for
another unit (72-2, 72-3; 82-4) in the group based on the token secret and the
password.

33. The system of claim 25, **characterized in that** the means for determining the check token in turn comprises

means for retrieving, at the first unit (32-1; 42-1; 52-2; 92-1), the token secret using the authentication token of the first unit and the password; and

5 means for creating, at the first unit, the check token for the second unit (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) based on the token secret and the password.

10 34. The system of claim 32 or 33, **characterized in that** the means for creating involves a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

15 35. The system of claim 25, **characterized by** policies implemented in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

20 36. The system of claim 25, **characterized by** further comprising means for generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

37. The system of claim 25, **characterized by** further comprising means for sending an authentication response message (34; 44; 94) from the second unit (34-2; 42-2; 92-4).

25 38. The system of claim 25, **characterized by** further comprising means for mutual authentication between two units (12; 22; 32; 42; 52; 72; 82; 92) in the group.

30 39. The system of claim 25, **characterized by** policies defining critical operations for which authentication is needed.

40. The system of claim 25, **characterized by** being a Personal Area Network (PAN).

41. A device (12; 22; 32; 42; 52; 72; 82; 92) belonging to a group (100) of at least two devices associated with a common password, and comprising means for password-based authentication, **characterized in that** this first device
5 comprises:

means for receiving a password;

means for assigning individual authentication tokens to other devices (72-2, 72-3; 82-4) in the group based on the password such that each authentication token is irreversibly determined by the password;

10 means for determining a check token for a second device (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) in the group based on the password and the authentication token of the first device (32-1; 42-1; 52-2; 92-1); and

means for transmitting the check token to the second device for authentication towards the second device.

15

42. The device of claim 41, **characterized by** further comprising

means for deleting the password and parameters generated in the authentication procedure except the authentication token after usage thereof.

20 43. The device of claim 41, **characterized by** further comprising

means for creating update information for the second device (42-2; 52-1, 52-3, 52-4; 92-4); and

means for securely transferring update information to the second device.

25 44. The device of claim 43, **characterized by** means for delegation of update rights to an intermediate device (92-2, 92-3), and means for sending update information for the second device (92-4) to the intermediate device.

30 45. The device of claim 41, **characterized in that** the means for assigning in turn comprises

means for determining a token secret common for the group (100) and non-correlated with the password; and

means for creating the authentication token for another device (72-2, 72-3; 82-4) in the group based on the token secret and the password.

46. The device of claim 41, **characterized in that** the means for determining
5 the check token in turn comprises

means for retrieving the token secret using the authentication token of the first device (32-1; 42-1; 52-2; 92-1) and the password; and

means for creating the check token for the second device (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) based on the token secret and the password.

10

47. A computer program product for, when executed by a computer, password-based authentication in a communication system comprising a group (100) of at least two units (12; 22; 32; 42; 52; 72; 82; 92) associated with a common password, **characterized by**

15 program means for assigning individual authentication tokens to the respective units of the group based on the password such that each authentication token is irreversibly determined by the password;

program means for determining, at a first unit (32-1; 42-1; 52-2; 92-1), a check token for a second unit (32-2; 42-2; 52-1, 52-3, 52-4; 92-4) based on
20 the password and the authentication token of the first unit; and

program means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.

25
